Summer 8-23-2019

Understanding the Dynamics of Unclaimed Terrorism Events in Pakistan: A Machine Learning Approach

Evan Christie

University of Maine, evan.christie@maine.edu

UNDERSTANDING THE DYNAMICS OF UNCLAIMED TERRORISM EVENTS IN PAKISTAN:

A MACHINE LEARNING APPROACH

By

Evan Christie

B.S. State University of New York Institute of Technology, 2008

A THESIS

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Arts

(in Global Policy)

The Graduate School

The University of Maine

August 2019

Advisory Committee:

Muhammad Asif Nawaz, Professor of History, Advisor

Kristin Vekasi, Professor of Political Science

Kate Beard-Tisdale, Professor of Spatial Information Science Engineering

UNDERSTANDING THE DYNAMICS OF UNCLAIMED TERRORISM EVENTS IN PAKISTAN:

A MACHINE LEARNING APPROACH

By Evan Christie

Thesis Advisor: Dr. Muhammad Asif Nawaz

An Abstract of the Thesis Presented
in Partial Fulfillment of the Requirements for the
Degree of Master of Arts
(in Global Policy)
August 2019

Terrorists thrive on media coverage because it multiplies the effect of an attack (Nacos, 2007). However, according to the Global Terrorism Database (GTD), only ten percent of terrorist attacks have been attributed globally from 1970 to 2017 (START, 2017). If the media coverage is a prerequisite for a terrorist group's survival, the lack of attributed attacks in the world is puzzling. This thesis examines the phenomenon of unattributed terrorist attacks using Pakistan as a case study. Pakistan is used as a case study because the percentage of claimed terrorist attacks in Pakistan closely resembles the global average of the lack of attribution of terrorist attacks – only fifteen percent of attacks are attributed in Pakistan. By using different organizational attributes – like attack, target, weapon preferences, spatial attack data, and lethality of attacks, this study attempts to match unattributed terror attacks to known groups.

ACKNOWLEDGEMENTS

I would like to express my most sincere gratitude to Dr. Asif Nawaz, my committee chair and mentor. He inspired me to work harder and challenge myself more than I thought possible by accomplishing academic research and pursuing this thesis. It was through his guidance, encouragements, and support that this thesis was possible, and I truly appreciate his patience and respect throughout the process. Thank you for pushing me to be the best I can be.

I would also like to thank my committee members, Dr. Kristin Vekasi and Dr. Kate Beard-Tisdale for providing excellent feedback and valuable suggestions on the improvement of this thesis. Thanks to you I was able to discover many new and interesting paths for my future education.

Finally, I would like to thank my family and my friends whose support made my education possible and gave me the ability to pursue my goals. Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

According to the Global Terrorism Database (GTD), claimed terrorist attacks have reduced over the last few years. Attacks are cheap and easy to claim and have a multiplying effect on the attack which provides benefits to the terrorist organization (Nacos, 2007). Yet, the GTD shows only 15 percent of global attacks have been claimed which suggests the claiming of attacks may not be as important to the act of terrorism as suggested by Nacos.

Even so, a compelling argument has been made my Kearns et al (2014) that suggests that attributions of attacks are significant and terrorist attacks should be studied in a way that goes beyond the binary notion of unclaimed versus claimed (Kearns et al, 2014). Their argument is supported by LaFree, Dylan, and Miller's argument that even without claims many attacks are attributed (LaFree, Dylan, and Miller, 2015) to different groups using characteristics of the groups. The GTD corroborates this by having 28 percent of the recorded attacks attributed to groups. The remainder of the attacks, however, are unclaimed and unattributed.

Even with the abundance of literature on terrorist organizational behavior and terrorist attacks, there are few scholars researching claimability. Fewer still research attribution, yet, the most common question after an attack is "Who did it?". The dearth of studies concerning claims and attributions likely prevents many studies from reaching their full explanatory ability.

Because most attacks go unclaimed, it is important to maximize the number of attacks that are attributed. This thesis aims to fill this gap in the current literature. By doing so, it will allow more robust studies on organizational lifespan, organizational behavior, and further the study of attribution of terrorist attacks to name a few examples. Additionally, this thesis will help further predict the perpetrators of attacks in Pakistan by using the group characteristics as indicated in historical attack data which has been collected by the GTD.

This thesis addresses the lack of attributed attacks in the GTD by creating an artificial neural network that leverages the data detailed in the GTD to make its own attribution predictions for unattributed terror attacks. The next section of this thesis covers the existing literature on claimability of terrorism followed by a discussion of artificial neural networks and how they are used. The following chapter covers the methodology of this study and details the data used and the specific details regarding the use of the artificial neural network as it pertains to this study. Subsequently, the next chapter is the analysis of the generated models and their accuracy and confidence after which will be a conclusion suggesting potential further areas of study and alternatives to make further study of attribution more successful.

CHAPTER 2

LITERATURE REVIEW

In this chapter, I first review a brief history of Pakistan. Then, I explore why some terrorist groups claim attacks, and examine the associated costs and benefits of doing so. Following this is an examination of current scholarship discussing how unclaimed attacks tend to go unclaimed when the costs outweigh the benefits. Next, I discuss how groups are able to be identified by their activities and how the attributes of a group can be used to make predictions about the groups. Finally, this chapter discusses the artificial neural network which is a technique used to take descriptive data and make classifications from the data.

2.1. A Brief History of Pakistan

Pakistan's efforts to survive as a country has been turbulent and filled with uncertainty (Ahmed, 1996). Despite that most of the Pakistani population is Muslim, Pakistan is composed of overwhelmingly diverse ethnic and linguistic groups which strongly identify themselves with their own ethnic groups. Major ethnic groups in Pakistan consist of Sindhis, Punjabis, Pashtuns, Muhajirs, Baloch, Kashmiris, Bengalis, Brahuis, and Saraikis and there are a few other minor ethnic groups. While English and Urdu are Pakistan's official languages, Pakistan has over 20 regional languages that are spoken by different ethnic groups. The most popularly spoken languages are Punjabi, Saraiki, Pashto, Sindhi, Balochi, Kashmiri among several other minority languages.

This divergence of peoples and language groups in Pakistan was one of the critical driving reasons that the country has been struggling to achieve a strong sense of nationalism given tension among ethnic groups continues to exist. When President

Iskandar Mirza led a military mobilization in 1958 and appointed General Ayub Kahn as Commander in chief, Pakistan was ruled by military rulers until 1971. In 1971 under President Yahya Khan, Pakistani Armed forces from West Pakistan led the suppression of East Pakistan and began genocide against Bengali (BBC, 2019). It became a full-scale civil war in Pakistan later known as the Bangladesh Liberation War. At the end of the war, East Pakistan became a separate country, current day's Bangladesh. After the Bangladesh Liberation War, Pakistan experiences two more military eras (from 1977 to 1988 and from 1999 to 2007) and two more democratic eras (from 1988 to 1999 and 2008 to present). Currently, Pakistan government is ruled by Prime Minister Imran Khan.

It is rare to find countries that are not ethnically heterogeneous. However, Pakistan is a country with ethnic, linguistic, religious diversity and the diversity in the country affected negatively on the establishment of high levels of polity and the security of the country. During 72 years of its history, Pakistan has been affected by conflicts caused by ethnic discord (Majeed, 2010). The conflicts in Pakistan range from territorial conflict between different ethnic groups to violent extremist groups in the country perpetrating attacks targeting civilians or military.

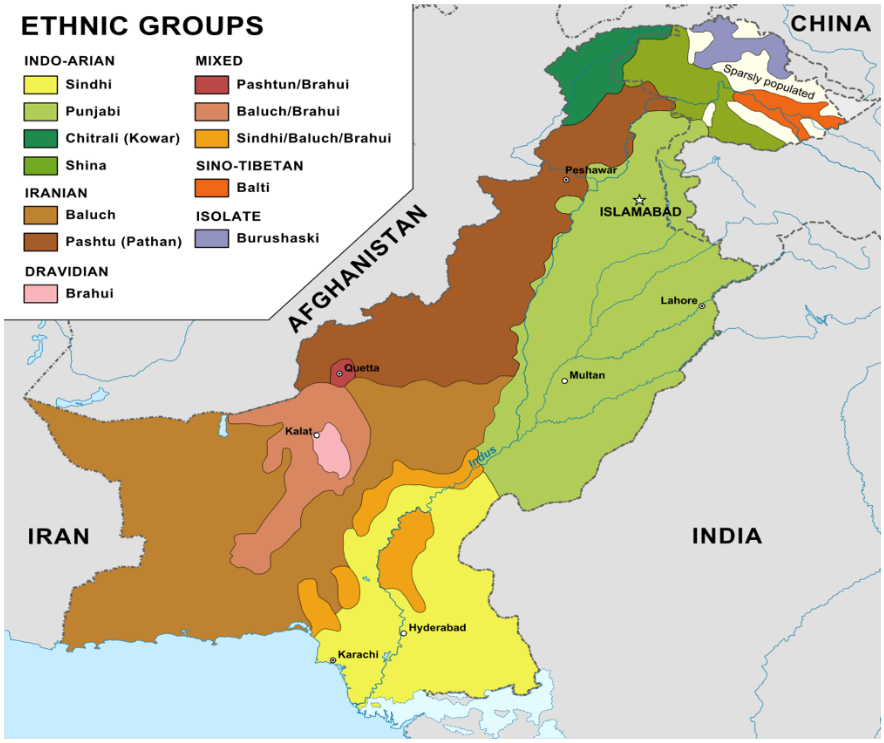

Figure 2.1. Ethnic Groups in Pakistan
Source: The University of Texas Libraries, The University of Texas at

As Figure 2.1. shows, Pakistan is composed of various ethnic groups. This ethnic heterogeneity led Pakistan to emerge as a country but failed to create nationalism (Jahan, 1972, as cited in Majeed, 2010) causing ethnic, and religious conflicts, on the basis of language, territoriality, and Caste (Majeed, 2010). In many cases, ethnic diversity led to competitiveness within the country among the groups (Smallbone, Kitching, & Athayde, 2010) in development of the region, representations in the government, sovereignty, allocation of resources, inter-province migration, and language and culture identity issues (Ahmed, 1996). For example, since Pakistan is composed of many linguistic groups, language is one of the ways that people identify themselves as a certain ethnic group. Suppression of Bengalis and the central government's policy to prohibit Bengalis to speak their language led to the separation of East Pakistan in 1971.

Violence and insecurity that are related to ethnic fractionalization are most prevalent in Sindh and Balochistan regions. The regions' economic demographic, social, political, and cultural trends have been shifting in consequences of ethnic clashes between ethnic groups and the central Pakistani government (Ahmed, 1996). In 1972, riots broke out in Sindh region against the central government which forced Sindhi people to speak Urdu. This demonstration led the central government to make Sindhi one of the official languages in Sindh region (Majeed, 2010).

In Balochistan, independence movements have been popular since 1947 when Balochi people were forcefully merged into Pakistan by the Pakistani ruling class (Laif and Hamza, 2009). Since 1972, Baloch politicians have been struggling to secure higher political positions in the majority of Urdu speaking central government (Majeed, 2010). Furthermore, when Pakistan discovered a natural gas depository as a source of energy, Balochistan was not able to get benefit from the gas pipeline, and to today still have minimum access (Laif and Hamza, 2009).

Ethnic conflict based on territory is most prominent conflict in Pakistan's Federally Administered Tribal Areas (FATA) region.

Figure 2.2. Federally Administered Tribal Areas (FATA)
Source: United States Institute of Peace

FATA is a territory covering about 27,500 square kilometers along the border between northwest Pakistan and southeast Afghanistan. This region is home to over 3.5 million Pashtun tribesmen and about 1.5 million refugees from Afghanistan (Nawaz, S., 2009). FATA has been a region of instability because of stronger ethnic identity than national identity. FATA zone was created in the 1800's by India's British colonial rulers when they realized that they were not able to control the mountainous region and its tribes militarily (Rupert, 2018). The British ended up letting the tribesmen rule themselves with an option to intervene if they acted against British colonizers' wills. As a result of this, ethnic Pashtun people who are religiously mostly Muslim, have been living in FATA at the border of Pakistan and Afghanistan loosely living by the British colonial laws. Since the end of colonial period, Pakistan has ruled FATA region through a mix of British colonial laws, military power, and government appointed representatives who receive the authority to rule the region (Abbas, 2014; Rupert, 2018).

Because of Pakistan's unique juxtaposition of ethnic groups, the country has been struggling to establish a strong rule of law and to keep the society stable. Instability of the country has been shown throughout the history of Pakistan as we discussed in conflicts in FATA region, secession of Bangladesh, and conflicts in Sindh and Baluchistan. However, internal conflicts are not the only reasons that cause instability in Pakistan. Pakistan has been home to terrorist groups such as al-Qaeda and Taliban. It became more obvious and known to the public that Pakistan has been involved in terrorism when the United States caught Osama bin Laden and assassinated him (Weinbaum, 2014).

The history of terrorism in Pakistan existed more than three decades ago, rather than abruptly triggered after the 9/11 like many other terrorist attacks in the middle east. The origin of Pakistani militant groups started as a method to counter the Soviet influence during the Soviet occupation of Afghanistan in the 1980s. To limit the spread of Soviet ideology in South Asia, American and Pakistani intelligence agencies supported the Mujahideen, who fights against non-Muslim forces (Yusuf, 2014). During this process, the Pakistan-Afghanistan border was not strictly monitored to allow militants to move across the border and conduct operations in Afghanistan. However, the freedom of controlling the Pakistan-Afghanistan border, which is the FATA, led to more severe instability within Pakistan after 9/11.

The FATA region has been the most contested territory between Pakistan and Afghanistan. Pashtuns are the majority of the population in FATA; about 15 million Pashtuns live in Afghanistan while 25 million live in Pakistan along the Durand Line[1]

[1] Durand Line is the 2,640-kilometer border between Afghanistan and Pakistan. It is the result of an agreement between Sir Montimer Durand, a secretary of the British Indian

(Nawaz, S., 2009; Tajik, 2014). Since the Pashtuns were separated by the artificial border drawn by the British, the people in FATA identify themselves as Pashtuns instead of Afghan or Pakistani. Furthermore, due to the poor border security in the FATA, it has been easy for Afghan Taliban leaders to recruit soldiers from Pashtuns. Taliban leaders used this tactic after the US invasion of Afghanistan to fight the outside forces (Nawaz, S., 2009). In an effort to monitor the border and minimize the effects of Taliban getting into Pakistan, Pakistan government launched a mission called "Operation Meezan." Although its purpose was to stop the influx of Pashtuns living on Afghanistan side of FATA to Pakistan, Pakistan military was told not to engage with Afghan Taliban and only arrest the others such as al-Qaeda members from Central Asia and other Arab countries (Haider, 2014; Nawaz, A., 2018). Because of communication issues between Pakistan government and the military, the operation ended in failure. Pakistan's effort to bring stability in the country and establish security has not been successful. Currently, there are still numerous terrorist groups operating within Pakistan and along the borders between Pakistan and Afghanistan.

In this thesis, I chose Pakistan as a case study for two reasons. First, Pakistan has many cases of active terrorist activities so there are a lot of data available to study from. Second, the trends of terrorism in Pakistan resembles the global terrorism trends which is represented in the Global Terrorism Database that I will use as the major data source in this thesis. Figure 2.3 shows the number of attacks and the number of kills by terrorist

---

government, and Abdur Rahman Khan, the emir, or ruler, of Afghanistan. The agreement was signed on November 12, 1893, in Kabul, Afghanistan. The British established the Durand Line after conquering the Pashtuns. 85% of the Durand Line follows the rivers and other physical features, not ethnic boundaries. It split the Pashtuns into two separate countries, Afghanistan, and Pakistan (Schons, 2011).

attack on a global scale from 1970 to 2018. We observe a fluctuation in the number of attacks and the number of kills by year from 1970 to 2009, and there is a sharp increase in the attacks and kills after 2010. Figure 2.4 shows the number of attacks and the number of kills by terrorist groups by year in Pakistan from 1970 to 2018. As we see in the global trend, the same trend occurs in Pakistan; there is a fluctuation in the number of attacks and the number of kills by year from 1970 to 2009, and we see a sharp increase after 2010. Since both global terrorism trend and the trend in Pakistan significantly resemble each other, the analysis on Pakistan will later be possible to generalize on the global terrorism trend.

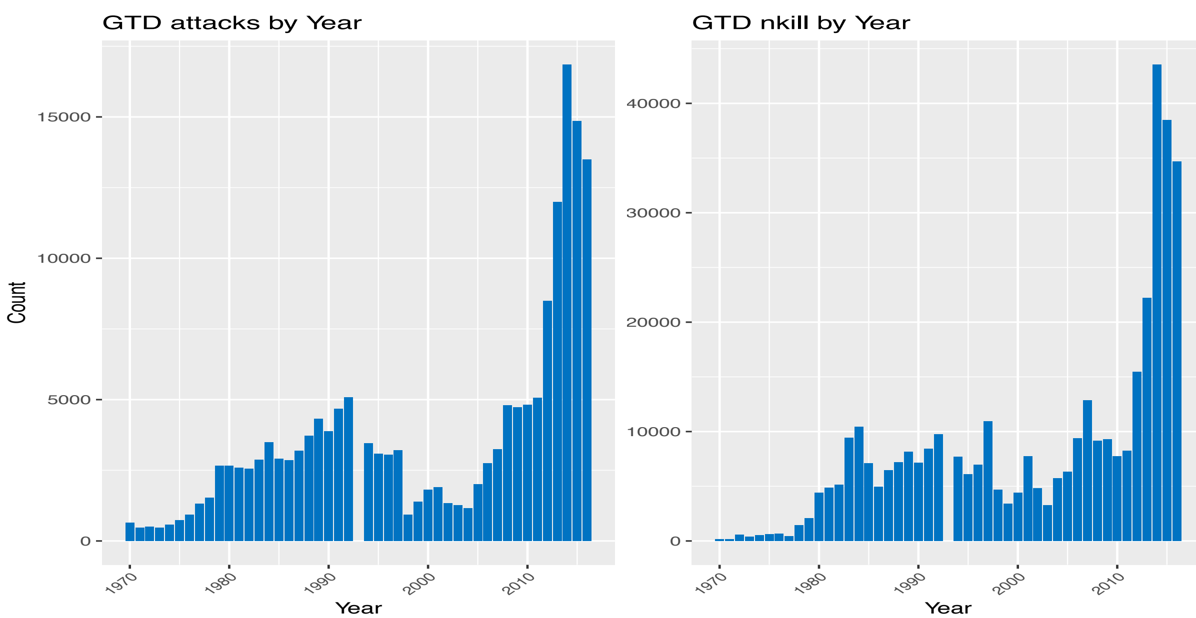

Figure 2.3. Global Trend: Number of Attacks and Number of Kills by Year
Source: Global Terrorism Database (GTD)

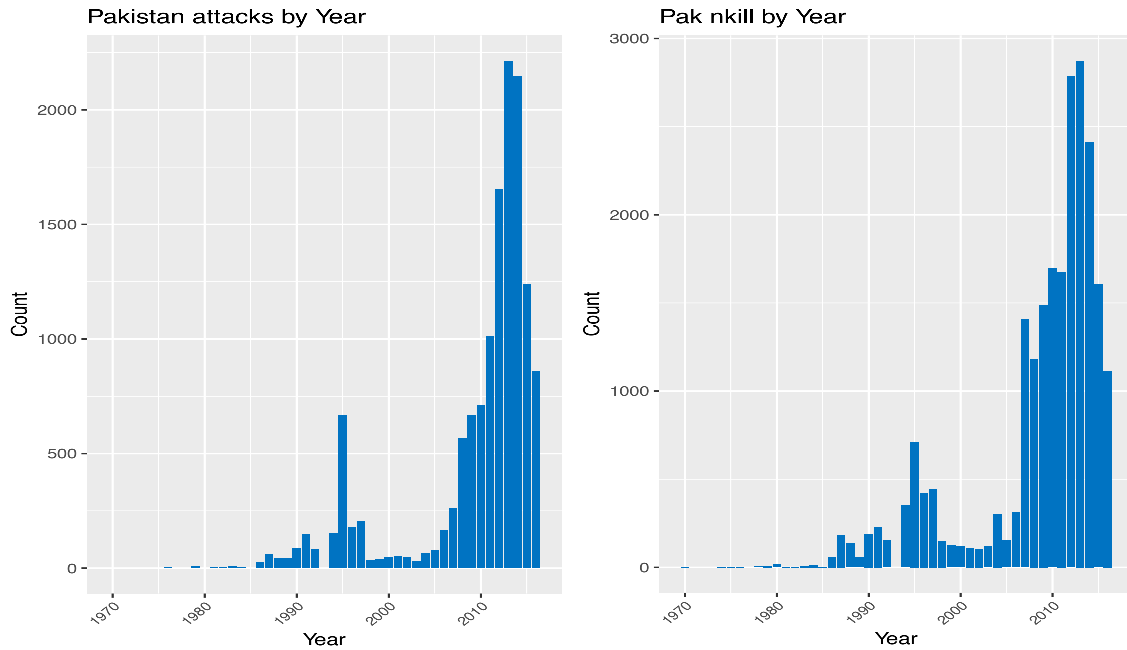

Figure 2.4. Pakistan Trend: Number of Attacks and Number of Kills by Year
Source: Global Terrorism Database

2.2. Why Groups Claim Attacks

There are a number of reasons why terrorist organizations claim attacks. Fundamentally, the definition of terrorism requires an attack to speak to a larger audience than the immediate victims of the attack itself and is in pursuit of a greater overall goal (Richards, 2014). If the intention of terrorist attacks is to speak to a larger audience as is common among most definitions of terrorism, then claiming attacks becomes the most effective way of spreading the message and is often done through media outlets. These media outlets then sensationalize the attack and the messaging behind giving greater attention to the perpetrators of attacks (Barnett & Reynolds, 2009). Nacos (2007) argues that "the inevitable and primary role of communication and propaganda is the terrorist design and the contemporary mass media's appetite to facilitate the need of virtually all terrorists to have their deeds publicized."

While the media is used to spread the message for the terrorist organizations, the message is used for the following reasons: competition among terrorist organizations, signaling strength, ideology, religion, and state retaliation (Wright, 2009).

For instance, intergroup competition among terrorist organizations sometimes dictates the decisions to claim or not claims attacks. The intergroup competition among terrorist organizations depicts situations in which there are multiple terrorist organizations all vying for the same resources (these resources being both monetary as well as masses of people who represent potential recruits). Hoffman (2010) argues when the number of terrorist organizations increases, the more difficult it is for actual perpetrators to distinguish themselves from groups that had not participated (Hoffman, 2010). To distinguishing themselves from less active gr5oups, terrorist organizations use claimed attacks to appeal to their audience to instill the idea they are the group to follow or support.

The second reason for claiming terrorist attacks is signaling strength. The signaling of strength is similar to competition among terrorist organizations with the exception that the signals are intended for other outside audiences. Outside audiences can be rival terrorist organizations, local and regional governments, or the pool of potential recruits for the group. By claiming a successful terrorist attack against a military target the group is able to project its power and tactical ability to not only its own audience but also as a message to governments that the group is strong and capable enough to achieve its goals (Kidd & Walter, 2006).

Claiming attacks can also increase the incitement for the ideological and religious goals of the terrorist organization in the local public. They are used to appeal to the idea that the act of violence is intended to further the ideological or religious goals of the group. In the case of religious motivations, the attack is done to benefit the religion and that it is the right thing to do. Hoffman (2010) and Drake (1998) both suggest that ideology and religion provide a motive and framework for terrorist organizations to act.

Lastly, claiming a terror attack is used to manipulate counter-terror responses from both the local and international governments. There are different ways in which claiming attacks affect counter-terror efforts. On one hand, terrorist organizations use the attacks in order to provoke a violent counter-terror response. The result of which would be the terrorist organization using the reprisal as a means of framing their conflict against an 'oppressive government' or 'the west.' On the other hand, eliciting a weak response from the government would have a similar effect of signaling strength and reinforce the organizations ability to provide better than the government. Still, terrorist organizations sometimes claim attacks perpetrated by other groups with the intention to outbid and increase the notoriety of the group (Kearns, Conlon, & Young, 2014).

These reasons for claiming attacks are represented by the strategic goals of organizations through the categories of intimidation, attrition, spoiling, outbidding, and provocation (Kidd & Walter, 2006). Intimidation represents the group's ability to punish and the local government's inability to stop the violence. Attrition is the group expressing its resolve by forcing itself and the government to pay higher costs (of life and material) over time. Spoiling is the act of terrorist organizations creating doubt and mistrust between two parties attempting to negotiate peace. Outbidding represents competition between groups for limited resources. Lastly, provocation is used to cause the government to overreact whereby the population becomes alienated and the terrorists cause becomes more appealing.

2.3. Why Groups Do Not Claim Attacks

Although claiming attacks yields benefits to terrorist organizations on certain occasions, numerous costs are also associated with claiming attacks. This is due to the organizational structure of terrorist groups. There is an assumption that the leadership of organizations is rational actors and they are conducting cost–benefit analyses when determining whether to claim an attack or not (Abrahms & Conrad, 2017). The core idea is that if the political impact outweighs the risks, then the attack is claimed; otherwise, it is not. For example, if a terrorist organization organized a bombing targeting occupation forces and was successful in the attack with minimal casualties then the attack is likely to be claimed. Conversely, if a similar attack is planned and many more innocent civilian women and children are killed then the attack is unlikely to be claimed. Max Abrahams elaborates on denial of organizational involvement. According to Abrahams, "many militant leaders have been reluctant to claim credit for civilian attacks due to the expected political fallout (Abrahams, 2018)." Abrahams uses the example of credit claiming by Taliban using the GTD. His studies show that leaders are more likely to not claim the attacks if the victims of the attacks are mostly civilians. Abrahams' analysis shows that among all the claimed attacks by Taliban, only 27% targeted civilians while 42% targeted government or military (Abrahams, 2018). As we can see in this example, Taliban claimed attacks when the victims were civilians who have politically influence. This phenomenon might be caused by the characteristics of Taliban as a terrorist organization which started as a Sunni Islamic fundamentalist political movement. Post 1990's, the Taliban had thousands of followers which was much larger than any political parties in Afghanistan (Dorronsoro, 2002).

Applying Abrahams' analogy of the chances of claiming attacks and the type of victims, I conducted analyses on all terrorist attacks in Pakistan.

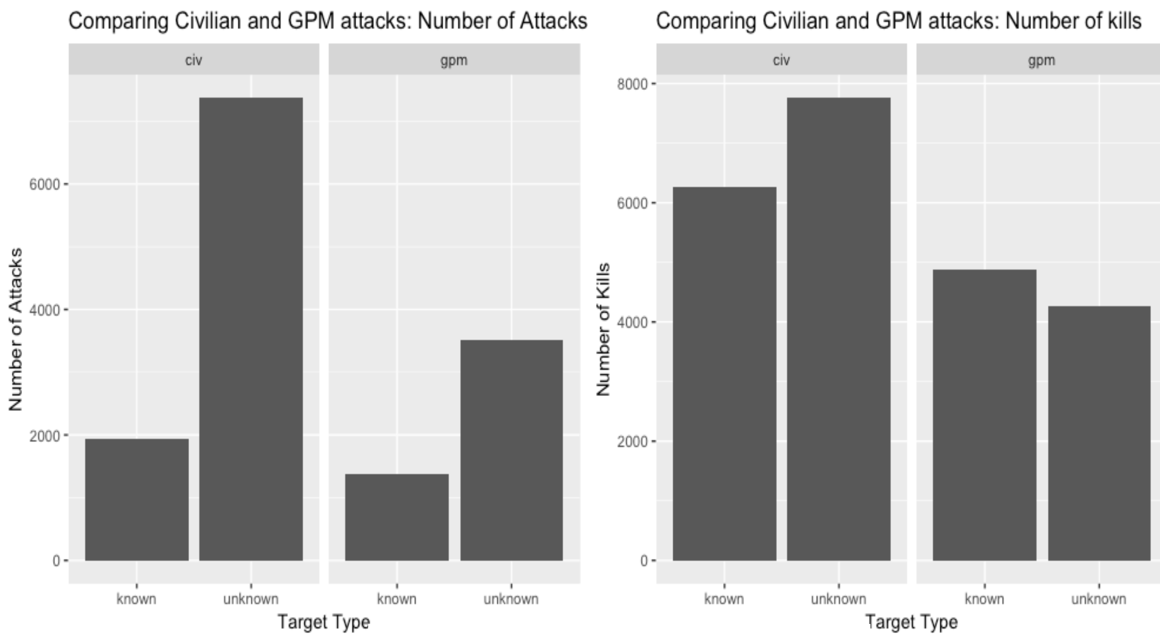

Figure 2.5. Civilian and GPM attacks

Figure 2.5 shows the comparison between civilian and government, police, and military (GPM) for number of attacks and the number of kills (lethality) of attacks. The number of known and unknown attacks for civilian surpass the number of known and unknown attacks for GPM attacks. Even though on average, civilians have been victims of terrorist attacks compared to GPM, there is a higher number of unknown civilian attacks than the attacks targeted at GPM. Therefore, Pakistan's number of attacks by terrorist groups follows Abrahams' argument on why terrorist groups do not claim attacks when the victims are civilians. On the number of kills, there are a greater number of kills for unknown attacks than known attacks when the victims were civilians. There are a greater number of kills for known attacks than unknown attacks when the victims were GPM.

There is a discrepancy when applying Abrahams' argument on less likelihood of claiming attacks when civilians are the victims. The reasoning comes from the fact that Abrahams uses claimed and unclaimed attacks while I use attributed and unattributed attacks. The difference between a claimed attacks and attributed attacks is as follows: claimed attacks are the ones that the perpetrating terrorist groups put out a formal media coverage claiming the attacks. Attributed attacks are the ones that the perpetrating terrorist group has been identified by a third party, such as multiple news organizations or witnesses, that the attacks have been done by a particular terrorist group. Furthermore, Abrahams uses the example of Taliban only while this thesis uses all terrorist attacks in Pakistan as a sample. At a basic analysis level, the Pakistan example in this thesis agrees with Abraham's argument; when the civilians are targeted as victims of terrorist attacks, it is less likely to be claimed and attributed. However, the reason that Taliban is less likely to claim attacks targeted to civilians because they are politically influential needs to be further examined in Pakistan example to fully understand why attacks are unattributed when they are targeting civilians.

Scholars suggest that while the leadership of terrorist organizations is normally synchronized and working towards the same goals, the regular members of the group are much more heterogeneous (Kearns, Conlon, & Young, 2014). The nature of this arrangement leads to the terrorist's dilemma as presented by Shapiro (Shapiro, 2013). In his book, *The Terrorist's Dilemma, he* shows this dynamic between leadership and members of the group where more control being exerted by the leadership over the members increases the risk of reprisal to the leadership of the group. Reprisals tend to come in the form of leadership decapitations conducted through drone strikes in recent years. The results of that introduce the concept of the principle-agent problem. The principle-agent problem highlights a situation that reduced control and communication from the leadership of terrorist organizations result in membership committing attacks and targeting populations that do not advance the goals of the organization.

Furthermore, many terrorist attacks go unclaimed because the attacks have failed to achieve their goal. Instead of signaling weakness, the attack goes unclaimed to prevent the terrorist organization from looking bad. Related to this, changing dynamics in public sentiment on the ground also has an impact on whether or not an attack is claimed. This could be due to successes in counter-terrorism efforts or even unintended consequences of attacks.

Regardless of the specific reasonings for whether an attack is claimed or not, the disparity of claimed versus unclaimed attacks as a significant problem. As we can see in Figure 2.6, the number of attacks that have been claimed globally is represented as only 9 percent while in Pakistan attacks are claimed 13 percent of the time.

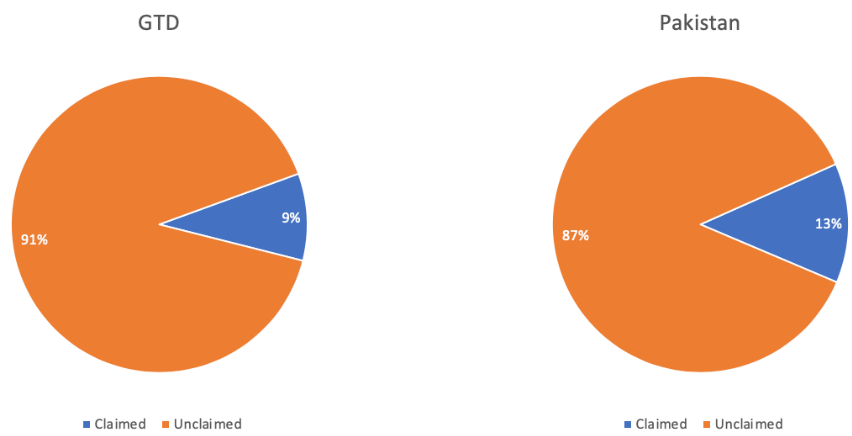

Figure 2.6. Global and Pakistan Claimed vs Unclaimed Attacks
(Data collected from the Global Terrorism Database)

With so much data concerning the claimed attacks missing from scholarly knowledge, it is difficult if not impossible to provide good counter-terrorism advice and produce accurate studies on specific group behavior. This is the gap in the data this thesis is attempting to fill.

According to Kearns, Conlon, and Young, each terrorist organization has a number of habits, patterns, or calling cards that separate the group from others (Kearns, Conlon, & Young, 2014).

2.4. Edge Cases: One Hit Wonders and Lone Wolfs

There are a couple of types of terrorist behaviors that will not be measurable through this thesis, however, they are still relevant and must be addressed. The first type of attack are attacks from typically smaller groups that only ever attack once or very rarely known as one-hit wonders (Blomberg & Engel, 2010). The Blomberg and Engel study shows that the majority of groups end up in this category; most groups commit between one and five attacks overall.

The second type of terrorism that this thesis won't be able to account for are lone wolf attacks. A lone wolf attack is where an individual, usually operates in their own nation's territory but separated from a terrorist organization, commits a terrorist attack and the individual claims to represent a terrorist organization. Examples of this are the multiple attacks in France and the San Bernardino shooting in the United States. Forster and Hader cite the Brussels and San Bernardino attacks to explain the way homegrown attacks increase operational security for the attack (Forster & Hader, 2016). This, in turn, reduces the likelihood the attack will be discovered ahead of time. Consequently, due to the nature of these types of attacks, there is often little attack data available or there are extremely loose connections between the individuals perpetrating the attack and the groups they claim to represent. Accepting the limitations of the edge cases, the Global Terrorism Database provides ample data describing attacks within Pakistan.

2.5. Terrorist Groups and Characteristics

Terrorist groups have unique characteristics that distinguish each group from others. They are fundamentally and strategically organized and operated differently from traditional definitions of criminal behavior. By observing the differences and the traits of terrorist groups, it is possible to sort out terrorist organizations. It is also possible to identify specific terrorist organizations' dependence on each group's behaviors, goals, and other characteristics they pursue.

To verify this claim, scholars have been studying ways to identify and classify terrorist organizations. Post, Ruby, and Shaw explain that the features of terrorist groups can and must be tailored to the type of organization, particular region or country involved (Smith, Damphouse, & Roberts, 2006) (Post, Ruby, & Shaw, 2002) (Ullah, Hussain, & Sajid,

2015) (Forster & Hader, 2016). In the research, they used five principle types of radical groups which are nationalist separatists, social revolutionaries, religious fundamentalists, nontraditional religious extremists, including “new religions”, and right-wing groups and evaluated individual group’s behaviors and indicators to categorize into the five types of radical groups (Hecht-Nielsen, 1988). Their research showed that groups that become terrorist organizations have similar characteristics which are group ideology and goals; experience with violence; authoritarian leadership and decision making; organizational processes such as recruitment, training, and attrition; and group psychological processes such as humiliation and need for revenge; and sense of threat and negative characterization of the enemy (Post, Ruby and Shaw, 2011). Furthermore, Smith, Damphousse, and Roberts did a similar study which categorizes terrorist groups and incidents into three types of domestic terrorism; left wing, right wing, and single issue (Smith, Damphousse, and Roberts, 2006). Their study found that terrorism involves people or groups that are motivated by political or social goals, ideological justification, and considerable forethought and planning (Smith, Damphousse, and Roberts, 2006). These specific characteristics are what the authors identified as unique strategies and characteristics of terrorist organizations compared to traditional criminality.

Studies by Post, Ruby, and Shaw and Smith, Damphousse and Roberts show that terrorist organizations behave differently from traditional criminals. Studies also indicate that terrorist organizations can be categorized by their behaviors, goals, and regions they operate. Therefore, it is also possible to recognize the unique behaviors of unidentified terrorist groups and make educated assumptions on which terrorist organization conducted specific attacks using artificial neural networks.

CHAPTER 3

METHODOLOGY

This chapter begins with exploratory analyses of the data used, then discusses the use of the artificial neural network to classify unclaimed terror attacks within Pakistan. It begins with a description of the variables used then continues with a discussion of the construction of the model.

3.1. Artificial Neural Networks

The neural network changes the typical computing model. In classical computing, we provide the computer with data and a set of rules, then the computer gives the answer. However, neural networks change the computing paradigm; once data and the answers are given to the neural network, it is left to "learn" the rules and patterns that connect the data to the answers. Figure 3.1 indicates the workflow of a neural network: each element will be discussed in detail.

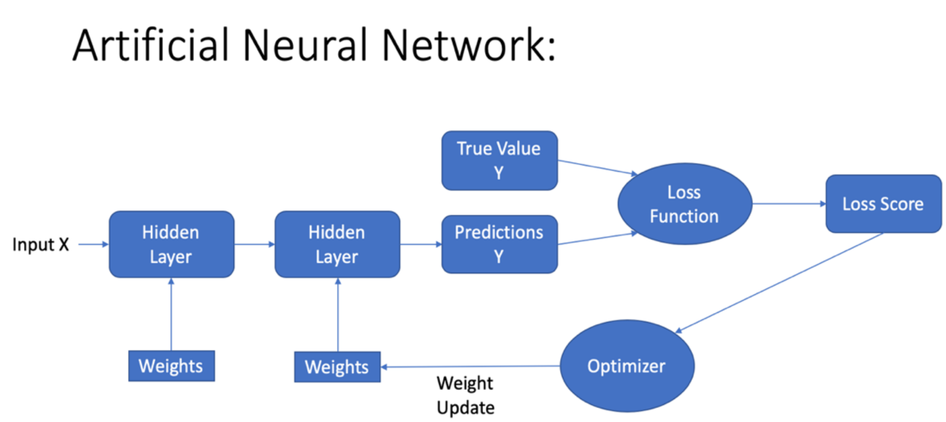

Figure 3.1. Flowchart of Neural Network

Neural Networks take preprocessed data and use weights to assign value to the various input variables. While artificial neural networks can accomplish tasks ranging from machine vision to image recognition, this thesis uses the network to accomplish multivariate classification (Hecht-Nielsen, 1988). The network takes in preprocessed data ensuring the data is normalized to make the learning easier for the network. That is, the data should have small values (ideally between 0, and 1) and be homogenous (have roughly the same range) (Chollet & Allaire, 2018).

Once the data has been vectorized and normalized, it is ready to be fed through the network. If we imagine the input data as a 2D matrix each input represents an entire row of data. A batch is a defined number of rows that have been input into the network. Lastly, an epoch represents the entire dataset of rows input into the network. For example, if there are 10,000 rows in the dataset and the batch size is set to 512, a batch is 512 rows being input and every 10,000 rows being input represents an epoch.

The next major pieces of the neural network are the layers and weights. These are typically represented as nodes with associated weights as seen in the following figure:

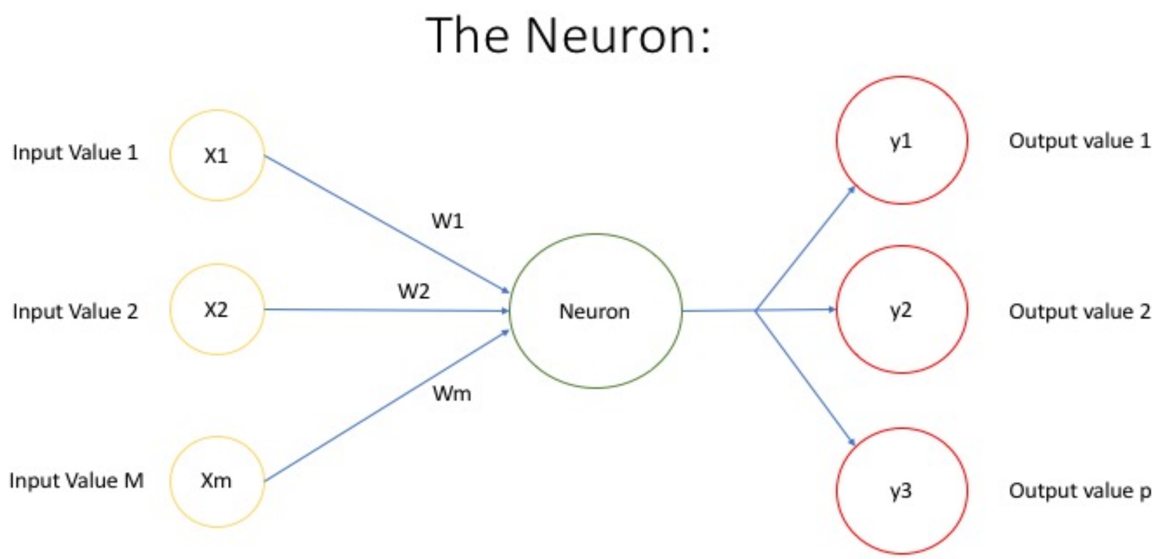

Figure 3.2. Example of a Node/Neuron

As seen in Figure 3.2, each node can have any number of inputs and any number of outputs. The only limitations are the input layer which will have a number of nodes that match the shape of the input and the output layer which will have a number of outputs that match the number of classification options (the dependent variable). Each neuron has associated with a weight for each incoming input and uses the weights, inputs, and an activation function to produce an output to send to subsequent nodes. The weights are all initialized by assigning them random values that are near 0. The activation functions are determined based on the type of data and results the machine is looking for. For this paper, the first two layers will use a rectifier function to produce outputs that represent the greater value of 0 or the input times weight.

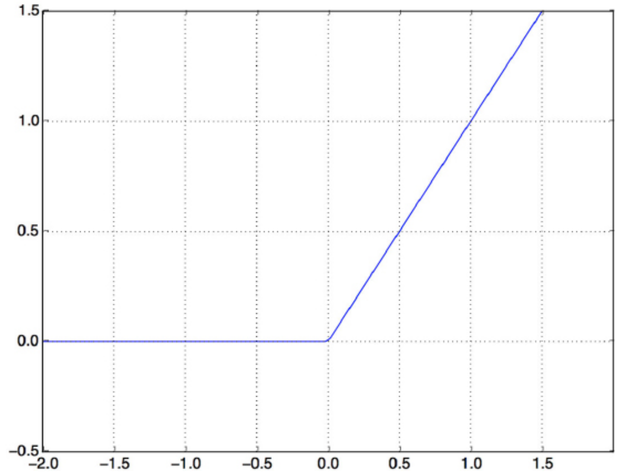

Figure 3.3. Rectified Linear Unit Function
Source: Chollet & Allaire, 2018

The final output layer uses a SoftMax activation function. The SoftMax function behaves like a logit function that has been generalized to produce a probability for each classification option with the restriction that all the probabilities sum to 1. For example, with classes labeled A, B, and C the SoftMax function may produce an output: A: 0.7, B: 0.1, C: 0.2. These outputs can be thought of as the network's confidence in each classification. The largest value ends up being the prediction for that set of inputs.

The network then uses a Loss function to calculate the difference between the predicted answer and the real answer. This is accomplished using stochastic gradient descent, where the function looks at the slope of the plane created by the loss function and tries to find the lowest point. This lowest point represents the least amount of difference between predicted answers and real answers.

After each batch, the optimizer function takes the current loss value and adjusts all the weights of the nodes in the network in an attempt to further minimize the loss score during the next batch. This cycle of feeding data, calculating loss, and updating the weights of the nodes is how the neural network 'learns' across the epochs of training data. Figure 3.4 displays the full network representation for this thesis.

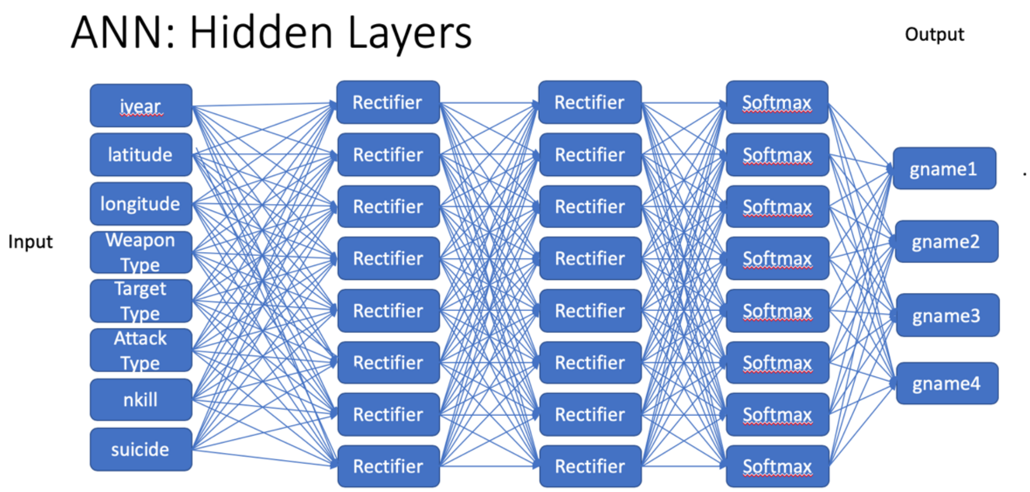

Figure 3.4. Structure of Hidden Layers

Once the model is finished being trained on the training data the test data is then input into the network. The test data then calculates an accuracy score for the model which represents the percentage of times the model was able to correctly predict the group that claimed the attack. After obtaining this score, the model is then measured against the validation set to benchmark the performance of this model. The model can then be fine-tuned as needed in order to increase the accuracy, however, each time the model should be tested against the validation set to simulate 'real world' improvements to the model.

Finally, once the model is sufficiently trained and validated the unknown attacks are then used as inputs to the model and the output will be the model's predictions for each unclaimed attack. In summary, the neural network takes the attribute data of each terrorist attack in Pakistan and makes a prediction of the group name that is most likely to have committed the attack.

3.2. Data

The data used comes from the widely used Global Terrorism Database (GTD). Although there are numerous definitions for terrorism the GTD defines terrorism as "the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation (START, 2018). Due to this definition the GTD uses three criteria for an event to be included in the database: (1) The act must be aimed at attaining a political, economic, religious, or social goal, (2) There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience than the immediate victims, (3) The action must be outside the context of legitimate warfare activities (START, 2018).

Since the case study is primarily concerned with Pakistan, a subset of the GTD is created to include only attacks that happened within Pakistan itself as coded by the GTD. The following independent variables are then selected to represent the behavioral patterns that different terrorist organizations within Pakistan exhibit. The following table indicates the summary statistics for the non-categorical variables of the known and unknown datasets.

Known Data	iyear	latitude	longitude	nkill	suicide
Observations	3152.00	3152.00	3152.00	3152.00	3152.00
Min	1976.00	24.60	61.58	0.00	0.00
Max	2017.00	36.15	74.83	158.00	1.00
Mean	2011.34	30.51	69.18	3.49	0.08
Std. Dev	5.65	3.63	2.74	9.34	0.28

Unknown Data	iyear	latitude	longitude	nkill	suicide
Observations	10654.00	10654.00	10654.00	10654.00	10654.00
Min	1970.00	24.73	61.58	0.00	0.00
Max	2017.00	36.34	76.12	90.00	1.00
Mean	2009.90	30.48	69.45	1.12	0.02
Std. Dev	6.98	3.71	2.50	3.24	0.15

Table 1. Summary Statistics

3.2.1. Independent Variables

I chose year, latitude and longitude, attack type, weapon type, target type, number of fatalities, presence of suicide bomber for independent variables. Below are the explanations and reasons why I chose them as my independent variables.

3.2.1.1. Year. First, Year is a numeric variable that is a measurement of the year the event took place. This variable controls for attacks that happen within group active periods. That is, if a group was active from 1985 through 1993 the network will be unlikely to predict that group to have committed an attack in 2016. When considering the year's impact on the reason's attacks are claimed, it has an effect on each one. Each attack whether pursuing the goal of intimidation, attribution, spoiling, outbidding, or provocation will have a temporal aspect to it.

3.2.1.2. Latitude and Longitude. Second, and third are latitude and longitude variables. They are both numeric and represent the geocoded coordinates of the city where the attack occurred. In order to keep as many data points in the dataset, for this thesis, the specificity attribute of the coordinates is ignored. The specificity variable accounts for instances where the exact coordinate is unknown and indicates which administrative level centroid is used to code the event. The result of the specificity is approximations that will still be useful for targeting information. These variables will control for the region of the country the group tends to target. This will help the network identify groups that tend to target specific regions in the country and is an important aspect of terrorist targeting decisions (Drake, 1998). Similar to the year variable, the location variables play an important role in furthering all goals because every attack will have a spatial component to it.

3.2.1.3. Attack Types. The fourth independent variable is the attack type. It's a categorical variable that represents the general method of attack for the event. The following options are recorded based on a hierarchy where, in the case of multiple methods, the preceding category will be recorded: Assassination, Hijacking, Kidnapping, Barricade Incident, Bombing/Explosion, Armed Assault, Unarmed Assault, Facility/Infrastructure Attack, and Unknown. This variable represents the preferred attack type of the groups with the assumption that groups tend to focus on types of attacks that reflect the goals of the group. The type of attack used speaks to the goals of the group. For example, when trying to intimidate a more lethal attack type may be used while pursuing attrition a softer attack type may be used. Further, when outbidding, there may be an increase in the violence of the type of attack in order to show strength. When pursuing the goal of provocation, attack type is less important.

3.2.1.4. Weapons Type. The fifth independent variable is the categorical variable weapon type. The variable records the main weapons used during the event. These categories are Biological, Chemical, Radiological, Nuclear, Firearms, Explosives, Fake Weapons, Incendiary, Melee, Vehicle, Sabotage Equipment, Other, and Unknown. This variable is intended to control for potential militancy of groups and holds the assumption that groups tend to use the same equipment over multiple attacks. Additionally, weapon types reflect how a group prefers to operate. For example, groups that prefer suicide attacks will have a tendency towards explosives instead of knives. Additionally, as Palfy indicates, weapon systems used by groups further a purpose. Groups will choose their weapon systems based on whether they are looking for lethality or fear for example (Palfy, 2003). As such, the weapon selection directly relates to the overall goals of the groups. Intimidation and outbidding should indicate different weapon selections as opposed to provocation or spoiling.

3.2.1.5. Target Type. The sixth independent variable is the target or victim type. It's a categorical variable that captures the general type of the target. The categories are Business, Government (general), Police, Military, Abortion-Related, Airports and Aircraft, Government (diplomatic), Educational Institution, Food or Water Supply, Journalists and Media, Maritime, NGO, Other, Private Citizens and Property, Religious Figures/Institutions, Telecommunication, Terrorists/Non-State Militias, Tourists, Transportation (other than aviation), Unknown, Utilities, Violent Political Parties. The variable indicates the goals and targeting priorities of the terrorist organizations as the assumption is that the groups will continue to attack the same types of targets that fit their organizational narrative and goals. This variable speaks loudest to the goals of provocation and intimidation where the groups would be targeting government, police, or military targets. Additionally, the target selection furthers the goals of spoiling by specifically targeting the groups or institutions coming to an agreement.

3.2.1.6. Number of Fatalities. Seventh, I use a numeric variable representing the number of fatalities for the incident. This number includes all victims and attackers who died as a direct result of the incident. This variable will control for the overall violence level of the groups. The assumption is that violent groups will have larger numbers of fatalities associated with their events and they will be involved in these violent events more often. The number of fatalities relates to all goals. For instances of intimidation, provocation, and outbidding a higher number of fatalities may seem appropriate. However, when pursuing the goals of attrition or spoiling, lower fatalities may be more prudent to the group.

3.2.1.7. Presence of a Suicide Bomber. The eighth and last independent variable is a binary variable that represents whether a suicide bomber was used in the event. This controls for groups that are willing to use suicide bombers to further their goals. The assumption for this variable is that not all groups need or are willing to use suicide bombers in their attacks and will help specify certain groups. Suicide bombers would be primarily used in pursuit of the goals of intimidation where the groups signal that they are absolutely committed to the cause. Additionally, suicide bombers would be most likely used to outbid opponents and to provoke extreme counter terror retaliations.

3.2.2. Dependent Variable

The dependent variable for this study is the categorical variable for the group name. This represents the official name of the group as recorded in the GTD. Additionally, the GTD dataset was further cleaned to remove events from the dataset that included generic group names that were not indicative of a professional group. Examples of coded group names whose events were removed from the dataset are youths, militants, and Mob.

3.3. Exploratory Analysis

In this section, I present exploratory analyses of the dataset. The purpose of the section is to see how the known data and unknown data resemble each other to show that the distributions of the training dataset is appropriate to apply to the unknown test sets. In this section, known data means the attacks that we know the perpetrator and unknown data means the attacks that we do not know the perpetrator.

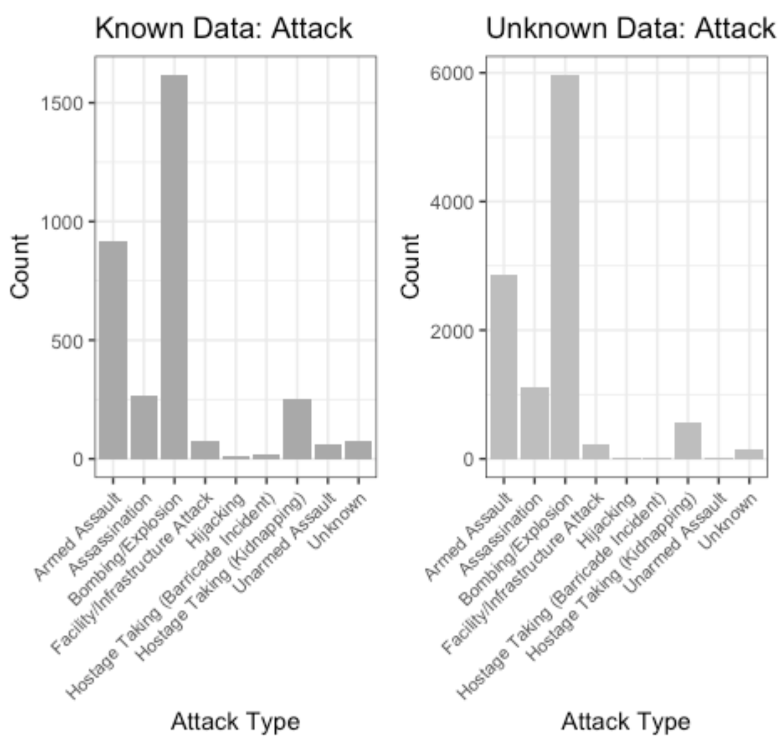

Figure 3.5. Attack Types

Figure 3.5 shows the attack types of known and unknown attacks. The left represents the known data and the right represents the unknown data. These two graphs resemble each other; both have a big number of Bombing/Explosion attacks followed by

Armed Assault and Assassination. Facility/Infrastructure Attack, Hijacking, Hostage Taking, Unarmed Assault, and Unknown have a relatively low frequency.

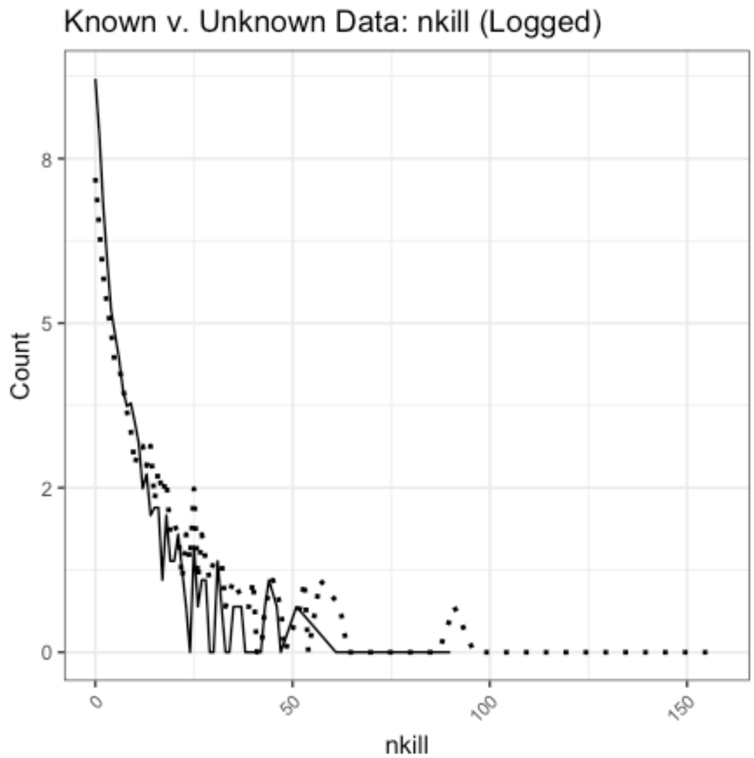

Figure 3.6. Number of Kills

Figure 3.6 shows the number of kills by known and unknown attacks. The dotted line represents the known attacks, and the solid line represents the unknown attacks. As we can see, the two lines almost overlap each other which means the training of known data can be appropriately applied to unknown data.

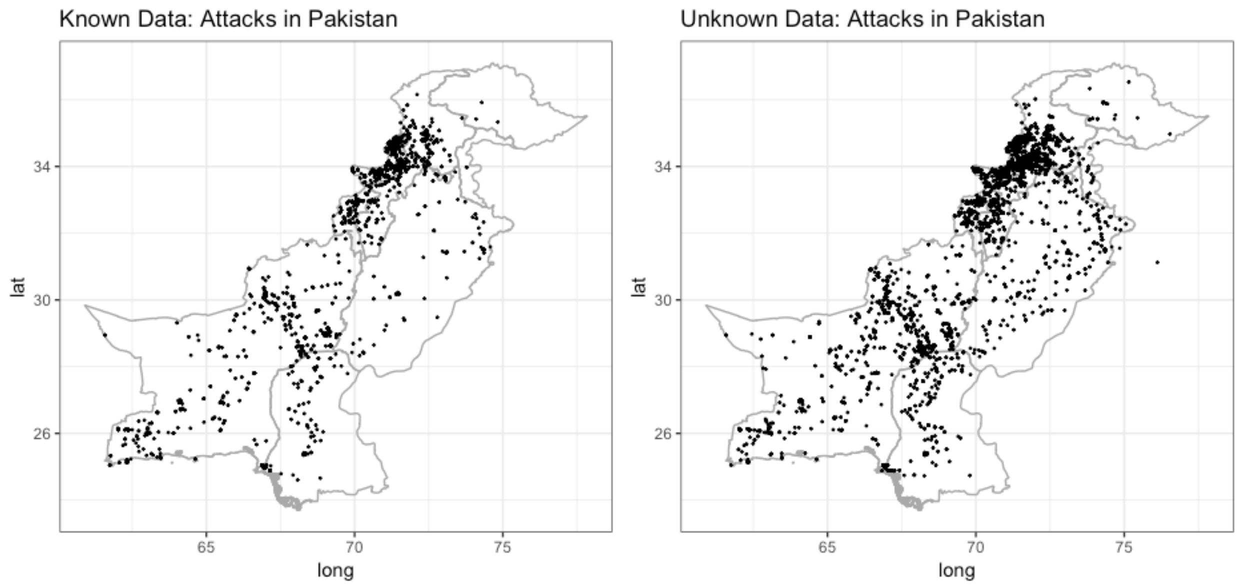

Figure 3.7. Locations of Attacks

Figure 3.7 represents the map of Pakistan with the places where attacks have happened. The left map shows the known data and the right map shows the unknown data. Though there are a lot more attacks represented in the unknown data, the regions where the attacks happen are similar. Therefore, the training on the known data will not be misleading to use to test the unknown data.

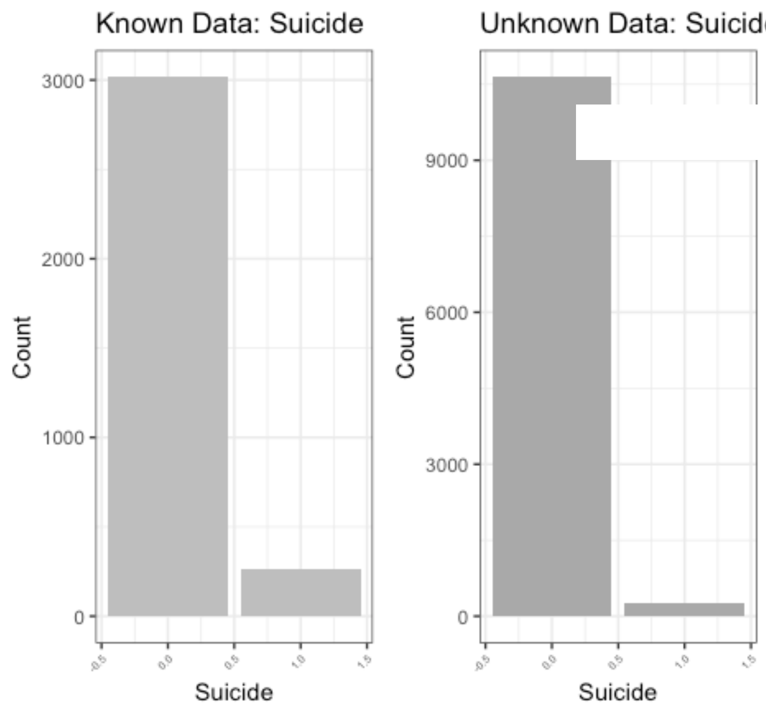

Figure 3.8. Presence of Suicide Attacks

Figure 3.8 shows the frequency of suicide attacks when terrorist groups commit attacks. Even though the number of suicide attacks are more than three times higher in the unknown attacks, the frequency of suicide attacks and the patterns of the suicide attacks are similar in both known and unknown datasets. Therefore, the known and unknown datasets resemble each other.

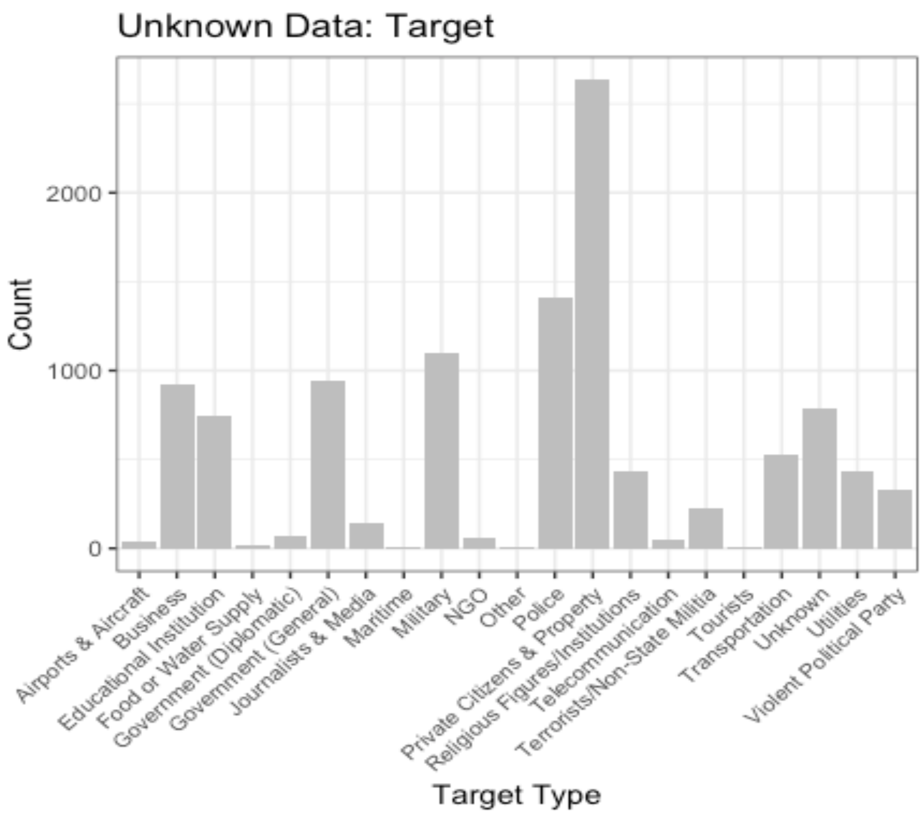

Figure 3.9. Target Type (Unknown Data)

Figure 3.9. and 3.10. show the target type of unknown and known datasets. Target types represent the locations where the attacks happen. Both known and unknown data have high frequencies of attacks against police and private citizens and properties. The known data also has a high frequency in attacks against military. Therefore, both known data and unknown data represent similar types of targets.

3.4. Processing Data and Creating the Model

Then the data is split into two sets: One where the attack has been attributed (has a group name value), and a second where the group name variable is Unknown. This results in a set of attributed attacks of 3,204 observations and unknown attacks of 10,891 observations.

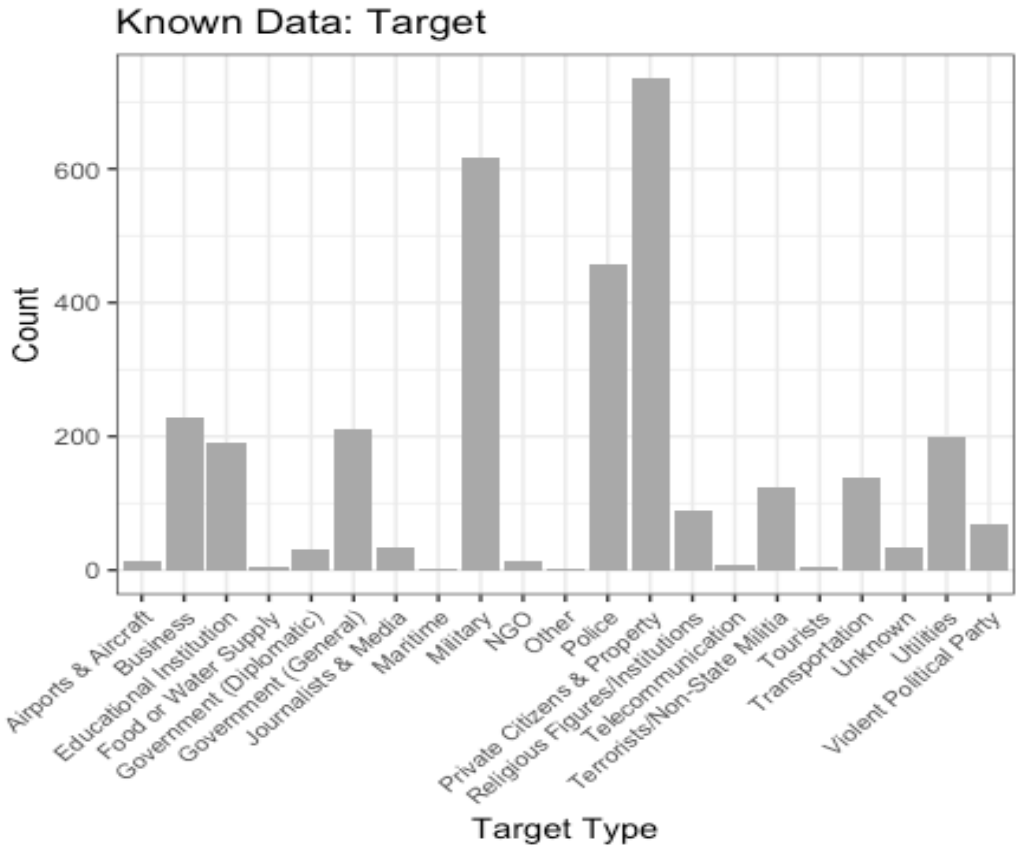

Figure 3.10. Target Type (Known Data)

The attributed dataset is then split into two different datasets using a 70/30 ratio with the new datasets being the training set having 70 percent, and the test set having 30 percent of the observations. After splitting, the independent variables are then scaled to make the learning easier for the machine. Additionally, the categorical variable for the group name is turned into a numeric value and is then one hot encoded into a large matrix of binary columns. For example, a three-value dataset of 'TTP', 'MQM', and 'BLA' will be given the numbers 1, 2, and 3. Then, columns in the dataset are generated to represent the binary categories of 'isTTP', 'isMQM' and 'isBLA' with a 1 representing true and 0 false.

The model is then initialized as a sequential model. First, an 8-node input layer is added using the rectifier activation function. Two hidden layers are then added with 45 nodes each also using the rectifier activation function. The model then has a final output layer with 95 nodes using a softmax activation function. Next, the model is compiled using a loss function of categorical cross entropy, the adam optimizer, and keeping a metric of accuracy.

The model is then fit using the training data and runs for 50 epochs with a batch size of 75. An epoch represents when every row in the dataset has been input into the network. The batch size represents the number of rows of data that are processed before the weights of the nodes are updated. The training dataset uses a validation split of .2 which represents 20 percent of the data are held back from the training data to be used in a validation test of the model. The ratio of training and test sets are typical.

Once the model has finished fitting. The loss and accuracy values are determined for both the training set and the validation set. Analyzing these numbers allows the determination of whether the model is acceptable or not. When the model is acceptable it is then fit on the remaining test set of data to get a measure of overall accuracy. Finally, the model is then used to make predictions on the completely unknown dataset where the network will assign a value to the likelihood of each dependent variable being correct for each row. The group name with the highest value will be the selected output for the given attacks.

CHAPTER 4

ANALYSIS AND CONCLUSION

This chapter will conduct an analysis of the training of the model followed by an overall conclusion and highlight areas of improvement in the future. Figure 4.1 shows the results from running the test and validation sets.

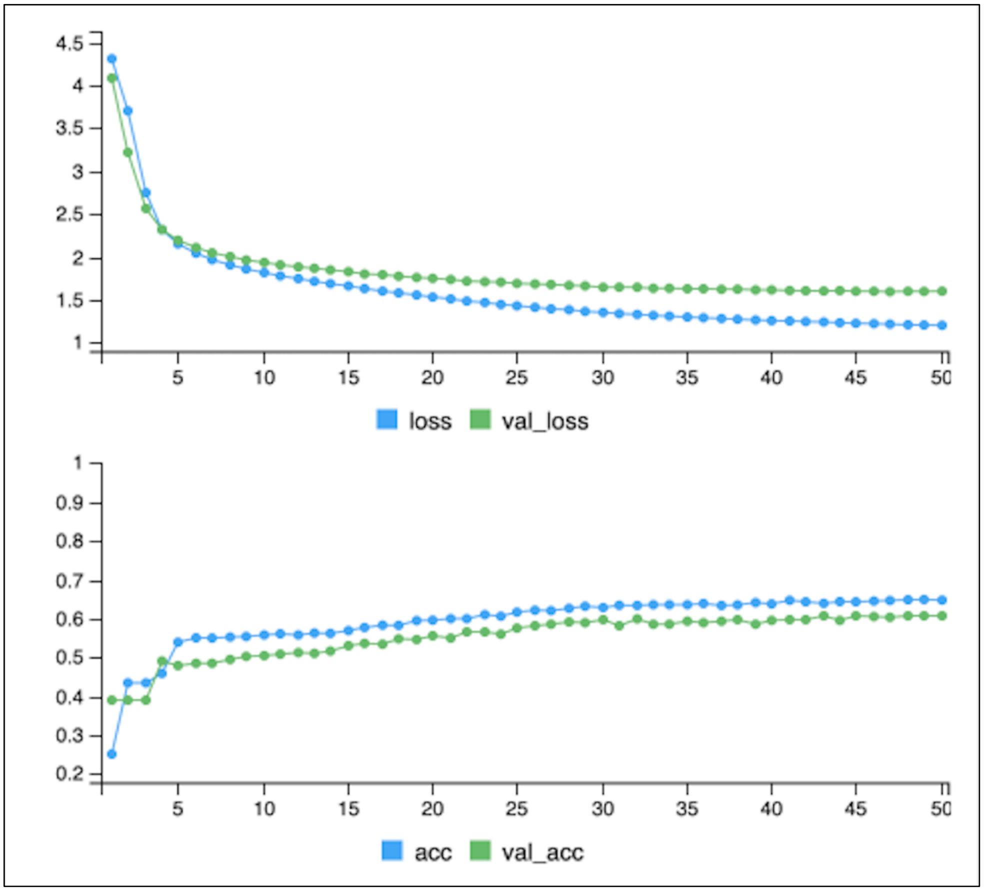

Figure 4.1. Top: Loss Score er Epoch; Bottom: Accuracy per Epoch

The results of the model training show a final loss value of 1.2033 and a validation loss of 1.617. The accuracy of the model is indicated as 65% and a validation accuracy of 61%. The closeness of the accuracy and validation accuracy over time indicate slight over fitting. Similarly, the validation plots stay relatively tight throughout the epoch with a slight exception towards the end of training.

Moving forward, future models can be improved by making a number of adjustments. First, the independent variables can be expanded from their current values to a deeper more nuanced version of the same variables according to the GTD. This has the possibility to increase variation between the attack type, weapon type, and target type variables between attacks resulting in potentially greater distinction between groups. Additionally, secondary and tertiary variables could be used for the attack, weapon, and target types. For example, using targtype2 or targtype3 for secondary and tertiary targets respectively. Lastly, adjustments could possibly be made to the compilation of the model. For example, the parameters of the model such as batch size, hidden layer depth, hidden layer width, and weight initialization can be adjusted to facilitate the gradual learning of the model over a longer period of time to prevent overfitting the training data. The impact of these suggestions should increase the overall accuracy of the model so that it can then be applied to unknown data with a greater degree of confidence.

To conclude, while the results of this neural network model achieved a 65% accuracy rate after being trained, I believe it can be improved on. Achieving results better than random chance indicates that the artificial neural networks can be used as a predictor of unattributed attacks. However, the success of the method is highly dependent on the model and the amount of data available. As such, this methodology may work better in areas of the world with higher numbers of attacks and lower numbers of groups. Equally plausible is that the methodology would likely perform worse in areas where there is little data to train a model with.

4.1. Limitations and Policy Implications of the Analysis

The major limitations of this study are the fact that the artificial neural networks can only predict and we cannot be 100% sure about the predicted results. As the accuracy of the model gets higher, the probability of the machine predicting the correct perpetrator will also increase, but it will still remain as a "prediction" rather than "the answer." Another limitation related to this is the cases of lone wolf attacks, one-hit-wanders, ghost groups, and imitation groups. It is difficult, if not impossible, to predict with this model whether the perpetrators were one-time action-oriented groups like lone wolf attacks and one-hit-wanders. Or, if the perpetrator groups were imitating certain famous and well-known groups in their attack strategies, group behaviors, and others distinct characteristics, then the machine will make a prediction of the original group that had more presence in terrorism history.

This study can be used by any governments and groups that work for counterterrorism. In this thesis, I show that machine learning can be used predict the perpetrators of unclaimed, unattributed terrorist attacks. The accuracy of model is still relatively low and will not be practical to be used yet, however, the accuracy is higher than random guessing. Therefore, with modification of the model and improvement in data collection, machine learning mechanism can be used to predict the perpetrators of unknown attacks in the future.

BIBLIOGRAPHY

Abbas, H. (2008, January). A Profile of Tehrik-i-Taliban Pakistan. *Combating Terrorism Center at West Point CTC Sentinel, 1*(2).

Abbas, H. (2014). *The Taliban Revival.* New Heaven and London: Yale University Press.

Abrahms , M., & Conrad, J. (2017). The Strategic Logic of Credit Claiming: A New Theory for Anonymous Terrorist Attacks. *Security Studies*, 279-304.

Barnett, B., & Reynolds, A. (2009). *Terrorism and the Press.* Ney York: Peter Lang Publishing Inc,.

BBC. (2019, March 4). Retrieved from Pakistan profile - Timeline: https://www.bbc.com/news/world-south-asia-12966786

Blomberg, S., & Engel, R. C. (2010). On the Duration and Sustainability of Transnational Terrorist Organizations. *Journal of Conflict Resolution*, 303-330.

Center for Global Education. (n.d.). Retrieved from A Political History: https://asiasociety.org/education/pakistan-political-history

Chollet, F., & Allaire, J. J. (2018). *Deep Learning with R.* Shelter Island: Manning Publication Co.

Dorronsoro, G. (2002). Pakistan and the Taliban: State Policy, Religious Networks and Political Connections. In C. Jaffrelot, *Pakistan: Nationalism without a Nation?* New Delhi: Lordson Publishers.

Drake, C. M. (1998). *Terrorists' Target Selection.* New York: St. Martin's Press Inc,.

Fair, C. C. (2009). Pakistan's Own War on Terror: What the Pakistani Public Thinks. *Journal of International Affairs, 63*(1), 39-55.

Forster, P., & Hader, T. (2016). Combating Domestic Terrorism: Observations from Brussels and San Bernardino. *Small Wars Journal*.

Hecht-Nielsen, R. (1988). Neurocomputing: picking the human brain. *IEEE Spectrum*, 36-41.

Hoffman, A. M. (2010). Voice and Silence: Why groups take credit for acts of terror. *Journal of Peace Research*, 615-626.

Hussain, S. E. (2010, May 17). Terrorism in Pakistan: Incident Patterns, Terrorists' Characteristics, and the Impact of Terrorist Arrest on Terrorism. *University of Pennsylvania Scholarly Commons*.

Jones, S. G. (2010). *Counterinsurgency in Pakistan.* Arlington, VA: RAND Corporation.

Kearns, E. M., Conlon, B., & Young, J. K. (2014). Lying About Terrorism. *Studies in Conflict & Terrorism*, 422-439.

Kidd, A. H., & Walter, B. F. (2006). The Strategies of Terrorism. *International Security*, 49-79.

LaFree, G., Dugan, L., & Miller, E. (2015). *Putting Terrorism in Context.* New York: Routledge.

Laif, M. I., & Hamza, M. A. (2009). Ethnic Nationalism in Pakistan: A Case Study Baloch Nationalism during Musharraf Regime. *Pakistan Vision, 10*(1), 49-81.

Majeed, G. (2010). Ethnicity and Ethnic Conflict in Pakistan. *Journal of Political Studies, 1*(2), 51-63.

Nacos, B. L. (2007). *Mass-Mediated Terrorism.* Plymouth: Rowman & Littlefield Publishers, Inc.

Nawaz, A. (2018). Modeling Terrorists' Targeting Selection: A Case Study of Taliban's Resilience in Pakistan (Working Paper).

Palfy, A. (2003). Weapon System Selection and Mass Casualty Outcomes. *Terrorism and Political Violence*, 81-95.

Post, J. M., Ruby, K. G., & Shaw, E. D. (2002). The Radical Group in Context: 2. Identification of Critical Elements in the Analysis of Risk for Terrorism by Radical Group Type. *Studies in Conflict & Terrorism*, 101-126.

Richards, A. (2014). Conceptualizing Terrorism. *Studies in Conflict & Terrorism*, 213-236.

Rupert, J. (2018). *Could Pakistan's Protest Undercut Taliban and Extremism?* United States Insitute of Peace.

Schons, M. (2011, January 21). The Durand Line. *National Geographic*.

Shah, S. W. (2012, January). Political Reforms in the Federally Administered Tribal Areas of Pakistan (FATA): Will it End the current Military? *Heidelberg Papers in South Asian and Comparative Politics*(64).

Shapiro, J. N. (2013). *The Terrorist's Dilemma.* New Jersey: Princeton University Press.

Smallborne, D., Kitching, J., & Athayde, R. (2010). Ethnic diversity, entrepreneurship and competitiveness in a global city. *International Small Business Journal, 28*(2), 174-190.

Smith, B. L., Damphouse, K. R., & Roberts, P. (2006). *Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preperatory Conduct.* Fayetteville: NCJRS.

Tajik, S. H. (2014). Counterterrorism Efforts of Law Enforcement Agencies in Pakistan. In M. Yusuf, *Pakistan's Counterterrorism Challenge* (pp. 103-126). Washington D.C.: Georgetown University Press .

The Commonwealth. (n.d.). Retrieved from Pakistan: History: http://thecommonwealth.org/our-member-countries/pakistan/history

Ullah, F., Hussain, B., & Sajid, I. (2015). Intelligence Aspects in Police Basic Training and Countering Terrorism in Khyber Pakhtunkhwa, Pakistan. *Pakistan Journal of Criminology*, 101-133.

Weinbaum, M. G. (2014). Militancy and Extremism in Pakistan: A US Perspective. In M. Yusuf, *Pakistan's Counterterrorism Challenge* (pp. 47-62). Washington D.C.: Georgetown University Press.

Wright, A. L. (2009). *Why Do Terrorists Claim Credit? Attack-Level and Country-Level Analyses of Factors Influencing Terrorist Credit-Taking Behavior.* Austin.

Yusuf, M. (2014). *Pakistan's Counterterrorism Challenge.* (M. Yusuf, Ed.) Washington D.C.: Georgetown University Press.

Yusuf, M. (2014). Pakistan's Militancy Challenge: From Where, to What? . In M. Yusuf, *Pakistan's Counterterrorism Challenge* (pp. 15-46). Washington, D.C.: Georgetown University Press.

BIOGRAPHY OF THE AUTHOR

Evan Christie was born and raised in Endicott, New York. He attended and graduated from the State University of New York Institute of Technology with a Bachelor of Science in Computer Science. He worked for 6 years and started his maters program in global policy and geographic information systems in 2016. Evan is a candidate for the Master of Arts degree in Global Policy from the University of Maine in August 2019.